CHAPTER 12

COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES AND FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE

A. COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS)

1. The Exon-Florio amendment to the Omnibus Trade and Competitiveness Act of 1988, as amended by the 1993 Defense Authorization Act, empowers the President to suspend, prohibit or dissolve ("block") foreign acquisitions, mergers and takeovers (hereafter, “transaction”) of "U.S. Persons." The Exon-Florio provisions (named after the statute's sponsors) are codified at Section 721 of Title VII of the Defense Production Act (DPA) of 1950, as amended. The President has broad authority to block a transaction under the statute if he determines the foreign interest acquiring control might take action that threatens to impair the national security. The statute provides that the President need not invoke his authority under Section 721 if provisions of law, other than Section 721 and the International Emergency Economic Powers Act, are adequate to deal with the national security issues of concern. In 2007, Congress passed the Foreign Investment and National Security Act (FINSA) of 2007. This Act amended Section 721 to improve U.S. security and clarify the review and investigative process under which the President may act.

2. To exercise his authority, the President must find that (1) there is credible evidence leading to the belief a foreign interest might take action to threaten or impair national security and (2) provisions of law, other than Exon-Florio and the International Emergency Economics Powers Act, are not adequate to protect the national security. The 1988 statute, as amended by the 1993 Defense Authorization Act, lists five factors that, "among others", should be taken into account in deciding whether an investigation should be conducted. These are:

a. Domestic production needed for projected national defense purposes;

b. The capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services;

c. The control of domestic industries and commercial activity by foreign citizens as it affects the capacity of the United States (U.S.) to meet the requirements of national security;

d. The potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country that supports terrorism is a concern regarding missile proliferation, or is a concern regarding the proliferation of chemical and biological weapons, or to a country that is on the Nuclear Non-Proliferation Special Country List or successor list; and

e. The potential effects of the proposed or pending transaction on U.S. international technological leadership in areas affecting United States national security.

3. The FINSA of 2007 added a number of additional factors to be considered:

a. The potential national security-related effects on U.S. critical infrastructure, including major energy assets;

b. The potential national security-related effects on U.S. critical technologies;

c. An assessment of whether the covered transaction is a foreign government-controlled transaction, as determined in the Act;

d. An assessment of the subject country's adherence to nonproliferation control regimes, including treaties, etc.; their relationship with the U.S. and record of cooperating on counter-terrorism efforts, etc.; and the potential for transshipment or diversion of technologies with military applications, etc.

e. The long-term projection of U.S. requirements for sources of energy and other critical resources and material; and

f. Such other factors as the President or the CFIUS may determine to be appropriate.

4. There is no mandatory requirement under the law for the company that is the target of the transaction or the foreign company to report a transaction. Nevertheless, the President or his designee may investigate a transaction at any time, including after a transaction has been concluded. Moreover, the transaction may be reported by a party not involved in the transaction. If a transaction was reported by the target company or by the foreign company, the President can reopen a case on the basis of material omissions or material misstatements in the original notice. Section 721 does not place any time limit on the President's authority to order divestment or other "appropriate" relief in such cases. Therefore, transactions involving companies engaged in business entailing classified information or advanced technologies tend to be reported since they could be expected to impact national security.

5. Other significant amendments to the Exon-Florio provision were made in the 1993 Defense Authorization Act. The first amendment mandates a formal 45-day investigation be commenced concerning any case in which an entity "controlled by or acting on behalf of a foreign government" is engaged in an acquisition that could affect national security. The second amendment statutorily bars foreign government-controlled entities from entering into a contract under a national security program, if the contract requires the company to have access to

"proscribed information." Proscribed information consists of Restricted Data, TOP SECRET, Special Access, Sensitive Compartmented, and Communications Security information. The Secretary of Defense and the Secretary of Energy are authorized to set aside this restriction (see section entitled “FOCI Related Matters” at the end of this chapter.

6. The 1993 Defense Authorization Act also requires an intelligence risk assessment be conducted concerning the possibility of diversions when the U.S. Company involved in the transaction is engaged in the development of technologies that are critical to national defense or are otherwise important to the defense industrial and technology base. FINSA requires the Director of National Intelligence to carry out these assessments and to incorporate the views of all intelligence agencies with respect to the transaction.

7. The FINSA expanded CFIUS membership by adding the Departments of Energy, Labor, and the Director of National Intelligence. Membership now includes the Departmental Secretaries or their designees of Treasury (Chair), Homeland Security, Commerce, Defense, State, Attorney General of the United States, Energy, Labor (nonvoting, ex officio), and the Director of National Intelligence (nonvoting, ex officio). Previous legislation or Executive Orders establishing CFIUS and its membership included adding the U.S. Trade Representative, the Council of Economic Advisors, the Office of Management and Budget, the Office of Science and Technology Policy, the Assistant to the President for National Security Affairs, and the Assistant to the President for Economic Policy. The heads of any other executive department, agency, or office, as the President determines appropriate are generally added on a case-by-case basis. The Services and other DoD Components provide input through the principal DoD representative, who is from the Defense Technology Security Administration (DTSA).

8. Once CFIUS becomes involved in the consideration of a possible transaction (as the result of a notification by the investors, on its own initiative, or at the request of a third party), it has 30 days to decide whether to initiate an investigation. The investigation must be completed not later than 45 days after its commencement, at which time the Committee must present a recommendation to the President. The President is required to render a decision within 15 days after completion of the Investigation. If the President decides to take action as the result of a CFIUS investigation, he must submit a written report to Congress on the actions he intends to take, including detailed rationale for his findings. The entire process may take up to 90 days to complete.

B. FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI)

1. General.

a. Any company bidding or performing on a contract requiring access to classified information must be granted a facility clearance (FCL) under the National Industrial Security Program **(**NISP**)**. To qualify for a FCL, the company is investigated to verify it has a reputation for integrity and lawful conduct. The company and its key officers must not have been barred from participating in U.S Government contracts, and certain of its officers and

directors must be eligible for personnel security clearances. As part of the FCL process, the company must execute a Standard Form (SF) 328, "Certificate Pertaining to Foreign Interests" and, for Department of Defense (DoD) contractors, a DD Form 441, "Security Agreement."

b. Completion of the SF 328 and the DD Form 441 are significant to the process leading to the granting of a facility security clearance that permits access to classified information. The SF 328 requires the company to answer a series of questions concerning possible foreign affiliation essential to the Government's assessment of the company's suitability to be granted access to classified information. The DD Form 441, a legally binding umbrella agreement between the company and the DoD, obligates signatory companies to comply with the U.S. Government's industrial security requirements prescribed within the National Industrial Security Program Operating Manual (NISPOM) (*reference z*). U.S. companies are also bound to the requirements of the NISPOM on a contract-by-contract basis by the Federal Acquisition Regulations (FAR) (*reference bbb*), Subpart 4.4, "Safeguarding Classified Information Within Industry," and the Security Requirements Clause at 52.204-2. (Also see Subpart 204.4 of the Defense FAR Supplement, "Safeguarding Classified Information Within Industry.")

c. The NISP generally does not govern access to controlled unclassified information. However, there are exceptions, such as companies cleared under one of several FOCI negation or mitigation arrangements. Moreover, violations of U.S. export laws and regulations by cleared companies, whether U.S. or foreign owned, could impact on their continued eligibility to possess a facility security clearance under the NISP. The increased risk accrues to cleared companies under FOCI and could compromise the integrity of classified and controlled unclassified information under a classified contract. As such, the NISP requires the establishment of an infrastructure and process to help ensure compliance with U.S. export laws and regulations concerning both classified and unclassified export-controlled information.

d. In addition to control of employee access to classified information, all companies cleared under the NISP must establish a program to control access by visitors to their facilities and visits by their employees to other facilities of other companies to ensure the protection of classified information. International visits must be in compliance with procedures similar to those established by the North Atlantic Treaty Organization (NATO). Records must be maintained of visits that entail access to classified information. A Technology Control Plan (TCP) must be developed by any cleared company that has long term foreign visitors on site or that has hired foreign nationals, to ensure they are insulated from classified work areas and information. This requirement may be waived if the company has other documented operating procedures providing for the same controls specified for a TCP. However, a TCP always is required for a company under certain FOCI arrangements**,** because it is presumed such companies will experience a greater number of visits by foreign owners or investors or their representatives, and may have representatives of foreign owners or investors involved in company management.

2. The Basics.

a. In keeping with longstanding U.S. Government policies, the NISPOM acknowledges it is in the interest of the United States to allow foreign investment in the defense industrial base where it is not inconsistent with U.S. national security interests. U.S. Government contracts requiring access to classified information may be awarded to companies under FOCI when adequate safeguards exist to protect national security interests. Within the context of the DoD, "national security interests" are information and technical data inherent in the development and production of military systems, such as system capabilities and vulnerabilities. If this knowledge is lost or compromised, potential adversaries of the U.S. would have the capability to duplicate or neutralize those systems. Another consideration from a security viewpoint is the potential of FOCI to disrupt performance of vital defense work.

b. The NISPOM states, in substance, “foreign interests must not have the power, by any means, to direct or decide matters affecting the management or operations of a company operating under a FCL if such power may result in the unauthorized disclosure of classified and controlled unclassified information, or may adversely affect the award or performance of classified contracts.” The acronym FOCI encompasses the possible avenues from which unauthorized foreign power may be exerted. When competent authority determines foreign interests have the power to exert control or influence, measures must be established to negate the FOCI or mitigate the associated risk.

c. When a company performing classified work is to be acquired by (or merge with) a foreign interest, an industrial security review is undertaken. The purpose of the review is to identify the elements of FOCI, evaluate the risks involved, assess whether a FCL should be retained or granted (in the case of a company sponsored for a FCL), and determine whether existing industrial security measures require enhancement in order to protect U. S. national security interests if an existing FCL is to be retained. The FOCI elements and the risks are considered in the aggregate, and the fact FOCI elements are present will not necessarily bar a company from receiving a facility clearance.

d. There are many components of foreign involvement requiring examination to determine whether a company is under FOCI and the extent of FOCI, such as those identified on SF 328. Documents other than the SF 328 are analyzed, to include filings with the Security and Exchange Commission (SEC) (for publicly traded companies), articles of incorporation, by-laws, loan and shareholder agreements, and other documents pertinent to potential foreign control or influence. In examining the source and nature of FOCI, the company's relationship with foreign persons, including (but not limited to) investors, directors, management, lenders, affiliates and customers is examined. Problematic FOCI can result from foreign ownership of a company, in whole or in part. FOCI could also be determined to be of industrial security significance if, for example, the U.S. company is indebted to a foreign interest, a significant portion of its income is derived from a foreign source, or the company is technologically dependent on a foreign interest.

e. The FOCI is then examined within the context of risk factors. These factors include the foreign intelligence threat, potential for unauthorized technology transfer based on published and intelligence reports, record of compliance by the potential foreign parent company with

laws, regulations, and contracts, and the nature of applicable international agreements between the U.S. Government and government of the potential foreign parent company. Pertinent agreements are security agreements, intelligence agreements, and law enforcement agreements. Cooperation by the other government in the areas of intelligence sharing and the sharing of law enforcement information also are important

f. If a company is determined to be under FOCI, and risks associated with FOCI are considered unacceptable, the company would be ineligible for a facility clearance or an existing clearance would be suspended or revoked, unless steps are taken to negate FOCI or mitigate associated risks to the satisfaction of the U.S. Government. The NISPOM prescribes various negation or mitigation arrangements available to address unacceptable levels of FOCI. The primary FOCI negation arrangements prescribed in the NISPOM are the Voting Trust (VT) and the Proxy Agreement (PA). The Special Security Agreement (SSA), the Security Control Agreement (SCA), the Limited Facility Clearance (LFCL), and the Board Resolution (BR) mitigate FOCI risks. The circumstances under which each FOCI negation or mitigation method is employed vary greatly.

g. The principal objective of each arrangement is to ensure there is no unauthorized access to classified and controlled unclassified information by foreign owners, their agents or representatives, or by other non-ownership derived sources of foreign control or influence. In this connection, the various FOCI arrangements enhance requirements governing the protection of classified information and unclassified export-controlled information required for any company performing classified work. The type of FOCI arrangement to be used in a particular situation is contingent on the analysis of the elements of FOCI reported or otherwise known and the analysis of the extant risk factors.

3. FOCI Negation and Mitigation Arrangements.

a. ***Voting Trust/Proxy Agreement.***

(1) The VT and PA are substantially identical arrangements whereby the voting rights of the foreign owners or shareholders (hereafter "shareholder") are vested with three cleared, U.S. citizen Voting Trustees or Proxy Holders (trustees) with the authority to operate substantially independent from the foreign owners. All three trustees are required to become members of the board of directors. The VT and PA provide Voting Trustees and Proxy Holders with substantially all prerogatives of ownership. In this respect, the power, authority, and responsibility of Voting Trustees and Proxy Holders differ significantly from that of Outside Directors under the SSA, as discussed below.

(2) Matters involving classified and export-controlled unclassified information are delegated to a special committee of the board of directors known as the Government Security Committee (GSC). The GSC is comprised of the trustees/proxy holders and officer/directors of the company. The company must appoint an individual to oversee visits and export control matters. The Facility Security Officer may be assigned this responsibility. The functions of the GSC are discussed in more detail later in this chapter.

(3) The foreign shareholder under the VT or PA is prohibited from being represented on the board of directors of the U.S. company. Voting Trustees and Proxy Holders may consult with the foreign shareholder concerning important business affairs of the U.S. company, but the shareholder has no *right* to be involved and no *right* to make decisions. There are notable exceptions, such as the filing of bankruptcy petitions and the prospective liquidation by the company. Contact with the company is closely scrutinized.

(4) The VT or PA can be employed ideally when the foreign shareholder, or group of foreign shareholders, is content with passive investment and does not desire active participation in the business management of the U.S. subsidiary. The VT or PA may be the only arrangement under which a company may secure a facility clearance when the foreign intelligence threat posture (or political considerations) of the parent company's government is problematic or the analysis of FOCI risk factors give rise to concern.

(5) A VT or PA also is appropriate under circumstances where a significant portion of the U.S. subsidiary's business entails access to “proscribed information," i.e., Restricted Data, TOP SECRET, Sensitive Compartmented, Special Access, and Communications Security information. Companies cleared under the VT or PA do not face impediments in the pursuit of classified contracts involving access to proscribed information because the company is legally insulated from its foreign owners. There are no restrictions on the types or sensitivity of contracts that may be awarded to the company.

(6) The VT or PA has also been employed when the foreign shareholder has only a minority stake and is not entitled to or does not desire to participate in the affairs of the U.S. company. The VT or PA may represent an attractive clearance method under circumstances of ownership or control by a foreign government.

(7) A TCP and enhanced security procedures are required, in addition to the GSC.

b. ***Special Security Agreement.***

(1) The SSA, like the VT and PA, is typically employed in cases of majority foreign ownership. There, however, the similarities end. The SSA is a FOCI *mitigation* arrangement -- the company is not insulated from the foreign owners or shareholders. The prerogatives of ownership for a foreign shareholder under the SSA are significantly broader than under the VT or PA. The foreign shareholder under the SSA retains the full panoply of rights and privileges of ownership *except* with respect to decisions involving classified and unclassified export-controlled information and related contracts.

(2) Under a SSA, the classified and unclassified export-controlled information must remain firmly under U.S. control--not the entire business enterprise. Thus, a principal difference between the VT or PA and the SSA is not whether involvement by the foreign shareholder is permitted, but whether a foreign owner has the *right* to a direct voice in *certain* business management decisions of the cleared U.S. company. Under the SSA, the foreign owner retains normal shareholder rights. Cleared or clearable U.S. citizens with no prior involvement with the company or its foreign parent, or any affiliated companies, are nominated for placement on the board of directors to serve as "Outside Directors." The

Outside Directors oversee and monitor compliance with U.S. security and export control laws and regulations. While three Outside Directors are typically appointed, the actual number considered necessary is determined on a case-by-case basis.

(3) The foreign owner or shareholder is permitted direct representation on the board of directors of the cleared company through the placement of "Inside Directors", who retain their normal rights as directors. As a general rule, Inside Directors are strictly prohibited from all business affairs of the company dealing with classified and unclassified export-controlled information. They have the right to be kept informed, to discuss, and to attempt to persuade other board members regarding the business affairs of the company concerning matters that come before the board of directors for deliberation and decision. Inside Directors may seek advice and counsel from the foreign shareholder and, as its representative on the board of directors; they may vote the wishes of the foreign shareholder consistent with their fiduciary responsibilities and the terms of the requisite SSA.

(4) The board of directors is comprised of the Outside Directors, the Inside Directors, and cleared U.S. citizen officer/directors of the cleared company. The number of Inside Directors must not exceed the combined total of Outside Directors and officer/directors. The chairman of the board and its principal officers must be resident U.S. citizens and the position of board chairman may not be filled by an Inside Director. The board must execute resolutions recognizing the SSA and its special obligations under the SSA, and other security resolutions as the DoD deems appropriate

(5) Matters involving classified and unclassified export-controlled information are delegated to a GSC as in the case of a VT or PA. The GSC in the case of a SSA is comprised of Outside Directors and officer/directors of the company. One of the Outside Directors is required to serve as chairman of the GSC. The company also must appoint an individual to oversee visits and export control matters. Inside Directors are prohibited from serving on the GSC.

(6) The SSA should be used only when it has been determined the government of the foreign parent has industrial security policies and practices substantially equivalent to those of the United States. FOCI mitigation under the SSA represents the best of both worlds. First, foreign shareholder representatives are at liberty to manage the company, except for portions of the business involved with classified and controlled unclassified information. Second, a company operating under the SSA may compete for all classified contracts *except* that eligibility for access to particularly sensitive classified work, i.e., "proscribed information," is not permitted without the written approval of the cognizant U.S. contracting authority with jurisdiction over the information involved. Access to proscribed information is predicated on the outcome of a "national interest determination", as described later in this chapter.

(7) Under the SSA, neither the foreign shareholders nor their proxies or agents, regardless of citizenship, are permitted access to classified information or influence over classified contracts in any manner whatsoever, except as may be provided under applicable U.S. laws and regulations (e.g., an export license or government approved visit request). Access to classified and unclassified export-controlled information may be permitted for a

representative of a foreign owner if the representative is a "lawful permanent resident alien or a protected individual" Subject to any contract restrictions. Where access to classified information is involved, the protected individual must possess an appropriate U. S. security clearance (if a U.S. citizen) or limited access authorization (if a foreign national), *and have a need-to-know for the information involved.*

c. ***Security Control Agreement.***

(1) The SCA is a tailored, mitigating arrangement, similar to the SSA. The SCA was established to fill a void where security was weakest--where foreign shareholders retain significant, but less than controlling, power and authority within cleared U.S. companies. Until the introduction of the SCA, some minority ownership cases were resolved by imposing the SSA under circumstances not warranting the access restrictions of the SSA. It was generally acknowledged that the use of security resolutions passed by the board of directors did not sufficiently mitigate problematic FOCI (See Board Resolutions, below). Consequently, too great a risk was assumed in some cases and unduly restrictive measures were imposed in other cases.

(2) Since control of the company remains in U.S. hands under the SCA, the vulnerability to inappropriate foreign influence is significantly reduced. With respect to classified contract eligibility, companies operating under the SCA are generally treated no differently than any other U.S. controlled entity, e.g., access limitations are usually not applied. A GSC is established, but normally only one Outside Director is appointed. In such case, the GSC would be comprised of the Outside Director, and cleared U.S. citizen officer/directors. The Defense Security Service (DSS), based upon the circumstances present, determines the number of Outside Directors considered to be necessary; in some circumstances none may be required. A facility security officer and export control official would work under the general supervision of the GSC.

(3) The SCA is usually considered for use where the minority foreign shareholder(s) holds sufficient voting stock to be represented on the board of directors of the U.S. company. However, this arrangement may be considered for use under circumstances totally unrelated to board representation, such as substantial foreign indebtedness or other avenues of foreign influence. As a practical matter, the SCA is most effective for cases falling just below the control threshold. For companies cleared under the security cognizance of the DoD, the DSS usually determines whether a company is under U.S. or foreign control.

d. ***Board Resolutions.***

(1) When a foreign interest does not own sufficient voting stock or is not otherwise entitled to representation on the U.S. company's board of directors, resolution(s) by the board is usually sufficient to mitigate FOCI. Board resolutions are also executed as part of the SSA and SCA. In such cases, the board identifies the foreign shareholder and, if applicable, the shareholder's representative(s) on the board. The board acknowledges the board member's obligation to comply with applicable U.S. laws and regulations, including the company's implementing security procedures and certifies the shareholder does not require, will not

have, and can be effectively precluded from unauthorized access to classified and controlled unclassified information.

(2) The resolution(s) must attest that the foreign shareholder will not be permitted to hold positions that may influence performance on classified contracts and attempts to do so will be reported promptly to appropriate, designated security authorities. Additional resolutions of the board of directors may be required by DSS when deemed appropriate. The Board Resolutions are executed initially and re-certified annually thereafter and distribution is made to key management officials of the company and the DSS on each such occasion.

e. ***Limited Facility Clearance***.

There are two types of limited clearances. They both require the imposition of limitations on the type and classification levels of information accessible by a company cleared under the arrangement.

(1) Limited Type One.

(a.) The first type of limited clearance is patterned after the "reciprocal facility security clearance" formerly granted pursuant to reciprocal provisions of bilateral Industrial Security Agreements. In some respects, this type of Limited Clearance replaces the "reciprocal facility security clearance", which is no longer used. Like its predecessor, the Limited Type One clearance enables a foreign-owned U.S. subsidiary to be cleared to perform on classified contracts awarded from the country in which the parent company is incorporated. Although not explicitly prescribed in the NISPOM, the clearance has been successfully applied to joint programs involving contractors of the participating governments (e.g., Medium Extended Air Defense System (MEADS)).

(b.) To qualify for a Limited Type One clearance, there must be an Industrial Security Agreement (and General Security Agreement, since the Industrial Security Agreement is an annex to the former agreement) with the government of the country or countries from which the FOCI emanates. Moreover, access to classified information must be limited to performance on a contract, subcontract, or program involving the foreign government(s), and classified information to be provided to the company must be determined to be releasable to the foreign government under National Disclosure Policy (NDP) guidelines (as determined by a Principal Disclosure Authority (PDA) or Designated Disclosure Authority (DDA)).

(c.) Since access to classified information is limited to classified contracts awarded from a parent company abroad or by the applicable foreign government, limited clearances are granted independent from U.S.-based procurement needs. The absence of a U.S.-based requirement to clear a company to perform on classified contracts distinguishes limited clearances from any other facility security clearance. A VT, PA, or SSA is not employed because the risks of unauthorized disclosure by virtue of ownership is not problematic, i.e., the information is determined in advance to be releasable to the foreign government(s) from which the ownership is derived.

(2) Limited Type Two.

(a.) The second type of limited facility security clearance is to be granted when the criteria for the Limited Type One clearance cannot be satisfied, provided there is a compelling need consistent with national security interests. This latter requirement has been interpreted to mean (and can be satisfied by) the conduct of a National Interest Determination (NID). It was intended that the Limited Type Two clearance would be applied when other clearance arrangements are found unsuitable or impractical, i.e., the clearance of last resort. The Limited Type Two facility clearance is subject to enhanced oversight by the DSS.

(b.) A foreign intelligence threat assessment is conducted, but the threat matrix is weighed against the need of the U.S. Government for the company's products or services. The NID process should be employed, regardless of whether proscribed information is involved, to assess the threat and to weigh the risk. The Limited Type Two clearance arrangement is only valid for the pertinent contract and the clearance is terminated following completion of the work.

4. Convergence of CFIUS and FOCI.

a. The CFIUS and FOCI processes are conducted in tandem, but they proceed on parallel and separate tracks, with different time constraints and considerations. If a U.S. company to be acquired by a foreign interest is engaged, or hopes to engage, in classified government contracts, the prospective investor must be able to successfully navigate both the CFIUS and FOCI processes. Indeed, these two very different processes have become inexorably linked, which is entirely appropriate. The CFIUS and FOCI review processes are complimentary in that they help ensure a more comprehensive governmental review.

b. While the CFIUS and FOCI processes have the preservation of the national security in common, they are both very different. Companies cleared by DoD are required by the NISPOM to report their possible acquisition by a foreign interest at the earliest practical time and DSS must be notified of any changes to the answers on the SF 328; notices filed with the CFIUS are voluntary. Moreover, reviews and investigations under Exon-Florio may encompass any transaction, whereas FOCI applies to classified information and contracts. Therefore, the scope of Exon-Florio and FOCI differ significantly; the latter focused on an important subset of national security concerns.

c. Under Exon-Florio, the President may only reopen a case on the basis of *material* omissions or *material* misstatements in the original notice. A FOCI case may be opened or reopened at any time for sufficient cause. Therefore, the threshold for reopening a FOCI case is significantly lower than exists under Exon-Florio.

d. Security arrangements proposed to negate or mitigate FOCI may assuage concerns arising during the CFIUS review process. Where classified information is involved (about 90-95 percent of all CFIUS cases), these arrangements are often the difference between a

transaction moving smoothly through the CFIUS review process and cases transitioning to investigation. The one occurrence where the CFIUS has recommended, or was positioned to recommend the President block a prospective acquisition, merger, or takeover of a cleared company can be attributed, in part, to the national FOCI policies.

e. Many of the same individuals within the federal bureaucracy are involved with Exon-Florio and FOCI acquisitions, mergers, and takeovers. When a prospective acquisition involves classified information, the FOCI and CFIUS reviews are increasingly converging into what appears to be an almost transparent dual process to individuals on the periphery. This trend is expected to continue.

5. FOCI-Related Security Matters.

*a. **Corporate Governance and the Government Security Committee.***

(1) Under the VT and PA, the GSC is comprised of Voting Trustees or Proxy Holders and officers/directors of the company. Under the SSA and SCA, the GSC is comprised of Outside Directors and officers/directors. The GSC is required to ensure the maintenance and implementation of security policies and procedures specified in the requisite FOCI arrangement, and all members obligate themselves in writing to exercise their best efforts to do so. Although the duties of GSC members are identified within the requisite FOCI arrangement, the extent of their involvement will necessarily vary depending upon the nature and extent of FOCI and the associated risk.

(2) While the duties of the GSC are defined by the applicable FOCI arrangement, these duties also must not conflict with general fiduciary principles assigned to the board of directors. For example, the position of Outside Director, although created by contract, e.g., the SSA, is nevertheless subject to fiduciary principles. The DSS model SSA obligates the GSC to maintain policies and procedures to safeguard classified and controlled unclassified information, to implement those policies and procedures, *and to exercise appropriate oversight and monitoring of U.S. subsidiary operations.* The provisions of the VT, PA, SSA, and SCA obligating or otherwise assigning duties to trustees and other members of the GSC are subject to reasonable and prudent interpretation and application on a case-by-case basis. The paramount consideration is whether the infrastructure and process exist to reliably ensure compliance by the company with those provisions.

(3) Trustees remain accountable for the overall security posture of the company, but it would be unrealistic to expect them to personally carry out security functions normally assigned to experienced subordinate officials in other cleared companies, such as the facility security officer or the technology control officer. While some trustees have taken the "hands on" approach, the degree of involvement by trustees should be thoughtfully considered within the context of need, general corporation law, and assigned functions under each particular security arrangement. Trustees are normally only infrequently on the premises of the cleared company.

(4) It is important to maintain ample records to help the trustees fulfill their important obligations. If those records do not exist, are not maintained, or key members of the management team are considered unreliable or untrustworthy, active involvement by one or more of the trustees should necessarily increase. Newly assigned Voting Trustees, Proxy Holders, and Outside Directors must not assume an effective security system is being inherited. The trustees should conduct a comprehensive review of the existing security system as soon as practicable upon assuming office.

(5) Many trustees must devote a significant portion of their time to protecting the economic interests of the shareholder by ensuring the success and growth of the U.S. company's business (a fiduciary responsibility). The special security obligations of trustees should not conflict with their fiduciary responsibilities as members of the board of directors.

b. ***Visits and Other Contacts*.**

(1) Chapter 6 of the NISPOM pertains to classified visits by contractor employees between or among cleared U.S. domestic contractors. Chapter 10 of the NISPOM pertains to international visits involving classified information or classified U.S. Government programs. The visitation requirements of Chapters 6 and 10 pertain to *all* companies operating under a facility security clearance, whether foreign owned or not.

(2) Chapter 6 requires records be maintained on *all* visitors approved for access to classified information. Moreover, procedural requirements to control the movement and activity of "long-term" visitors temporarily assigned to the facility are also set forth in Chapter 6. Chapter 10 requires the establishment of procedures to monitor international visits and assignments of foreign nationals, both employees and visitors; records must be maintained of foreign national visitors. In recognition of the increased risk of deliberate or inadvertent access to classified and unclassified export-controlled information by foreign national visitors and employees, Chapter 10 requires a TCP be prepared.

(3) From the inception of the FOCI arrangements, it was presumed companies under FOCI would experience increased visits and other forms of contact with foreign shareholder representatives, i.e., an opportunity to exert unauthorized influence or gain access to information to which they are not entitled. Consequently, visit and contact procedures were often required for FOCI companies exceeding those normally applied to other cleared companies, i.e., the requirements contained within Chapters 6 and 10 of the NISPOM. The enhanced procedures were included in FOCI negation and mitigation arrangements to mitigate associated risks.

(4) Enhanced procedures for the regulation of visits and contacts with foreign shareholder representatives has been integral to the VT and PA since the inception of those security arrangements in 1955 and 1978 respectively. Enhanced procedures governing the regulation of visits and contacts were incorporated within the SSA upon its creation in 1983. These procedures typically include screening and approval by the facility security officer and/or a member of the GSC.

(5) The enhanced visitation procedures embodied under FOCI negation and mitigation arrangements are unique because, unlike the requirements of Chapters 6 and 10, (a) they are limited to the foreign shareholder (and entities controlled by the shareholder), and (b) they are designed to prevent the shareholder from exerting influence over the business management of the company. Foreign influence over the business management of companies cleared under the VT or PA is severely restricted. Foreign shareholder influence over the business management of companies cleared under the SSA and SCA is also restricted, but to a significantly lesser degree.

(6) The contact reporting requirement is contained within the VT, PA, and the SSA. The requirement was developed to screen contacts with representatives of the foreign shareholder and its affiliates in order to identify possible inappropriate or questionable behavior concerning "regulated" activity under the requisite FOCI negation or mitigation arrangement and to conduct a follow-up examination if necessary. The requirement encompasses all contacts by any means with cleared and non-cleared persons, regardless of citizenship, who may be acting, directly or indirectly, for or on behalf of the foreign shareholder, regardless of where the contact occurs.

(7) Under the SSA, for example, regulated activity concerns matters under the jurisdiction of the GSC, that is, unauthorized (or attempted) access to classified and unclassified export-controlled information *and* unauthorized involvement with classified contracts. Under the VT and PA, regulated activity includes matters for which the GSC is responsible *and* the insulation obligations of Voting Trustees and Proxy Holders unique to those two arrangements.

(8) A post-contact requirement is also contained within the VT, PA, and SSA. The requirement consists of written reports of "after the fact" contact with foreign shareholder representatives involving "strictly social" contact. Post-contact reporting was not made a standard element of the VT, PA, and SSA until 1993. A controversial and unsuccessful acquisition attempt in 1992 served as the catalyst for the post-contact reporting requirement.

c. ***National Interest Determination.***

(1) The NISPOM specifies, "a determination to disclose proscribed information to a company cleared under an SSA requires the rendering of a favorable National Interest Determination be rendered prior to contract award." Proscribed information consists of Restricted Data, TOP SECRET, Special Access Program, Sensitive Compartmented, and Communications Security information.

(2) A favorable NID consists of a determination by a senior official that there is "compelling evidence that release of such information to a company cleared under the SSA arrangement advances the national security interests of the United States." The authority to make this decision is assigned currently to an official at the “Program Executive Office” level. The approval authority was set at a senior level to guard against contract awards that might reasonably be considered contrary to national security interests and to ensure a fair and

impartial decision was rendered. Senior level approval also serves to establish accountability for those decisions.

(3) The contracting agency sponsoring a NID must provide, inter alia, the following information to the NID approval authority (Section 2-309b of the NISPOM):

(a.) The identification of the national security interests involved and the ways in which award of the contract helps advance those interests;

(b.) The availability of any other U.S. company with the capacity, capability, and technical expertise to satisfy acquisition, technology base, or industrial base requirements and the reason any such company should be denied the contract; and

(c.) A description of the alternative means available to satisfy the requirement, and the reasons alternative means are not acceptable.

(d.) Prior to the advent of the NID process, cleared companies, wholly or majority foreign owned, were generally granted access to proscribed information under a VT or PA. The NID was established as an element of the SSA to allay concerns with respect to what many agencies considered the "family jewels", i.e., the most sensitive information in their inventories. These agencies simply would not support release of what became known as proscribed information to majority foreign owned companies unless they had the opportunity, on a case-by-case basis, to deny such releases at a high level. Hence, approval of the NID process served as the catalyst for approval of the SSA arrangement.

d. ***Technology Control Plan.***

The primary purpose of the TCP is to prescribe the access controls and protective security measures necessary to preclude unauthorized access, to include inadvertent access, by long-term foreign national visitors and foreign national employees to classified and export-controlled unclassified information at cleared contractor facilities. The TCP includes, as necessary, such procedures as unique badges for foreign nationals, segregated work areas, and enhanced security indoctrination. Under the provisions of individual FOCI arrangements, a TCP is prepared and implemented under the general auspices of the GSC. See Chapter 7 for a discussion of the TCP.